

AKO “Single Email” and the Army Enterprise Architecture Applications



AKO Directory Services

- **Single email lessons learned**
- **What is relationship between single email and directory services?**
- **What are Directory Services and the AKO Directory?**
- **Why use the AKO Directory?**
- **How does a user and an application interface to the AKO Directory?**
- **What does this mean for the “Joint” environment?**

Single email Lessons Learned

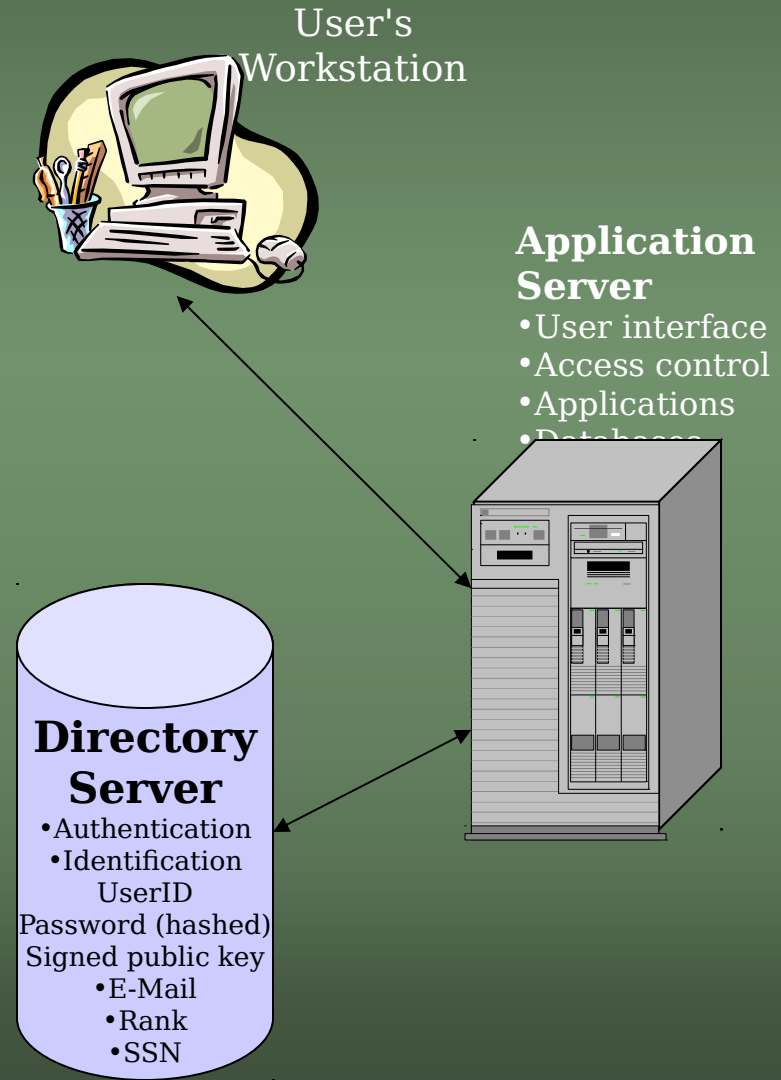
- **Web-mail is still a couple of years behind in functionality from client-based mail**
- **Architecture of large single email system must be carefully thought out. Collaborate with others that have implemented not just the software vendor.**
- **Scale and security are non-negotiable. But functionality will be never ending thorn.**
- **Comms pipes can't be wished away**
- **Having the capability of lifetime email address is very powerful**
 - **DFAS travel vouchers**
 - **Loan repayment program**
 - **Targeted email messages**

What is relationship between single email and directory services?

- **Simply --- the single email account is tied directly to our single directory**
- **There is one account for each person that does not change throughout their career**
- **The single directory is tied to the Personnel system --- thus when someone departs service after 4 year tour; their account can be deactivated in one place for all services.**
- **Eventually --- will have meta-directory to connect master directory to the Microsoft Active Directory**

What are Directory Services?

- **Directory Services Provides:**
 - User authentication
 - User identification
 - Single point of look-up for user properties, e.g.:
 - Name
 - Rank
 - SSN
 - E-mail address
 - Location
 - Organization
 - Signed Public Key (PKI)



How are Directory Services Implemented?

- **Authentication Transaction Process**
 - Web application prompts user for authentication credentials
 - Web application passes credentials via LDAP to Directory
 - Directory returns user's identity (Distinguished Name) for successful logons
- **User Property Lookup Transaction Process**
 - Web application requests field value for a user via LDAP from the Directory
 - Specify user's DN
 - Specify Directory field name
 - Directory returns field value
 - Restricted fields require special permissions for application to be able to access

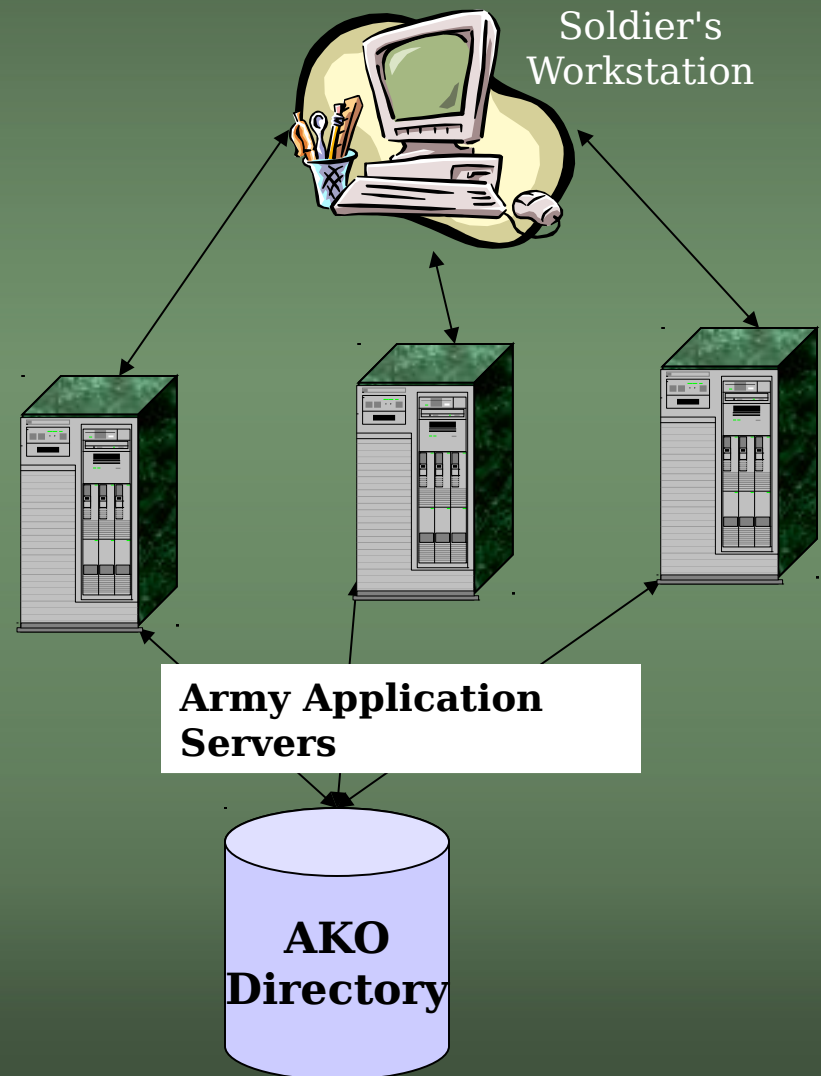
Note that all requests are implemented as transactions between the web application server and the AKO Directory Server

What is the AKO Directory?

- **Single Authentication and Identification Authority for the Army**
 - Active
 - Reserve
 - Guard
 - Civilians
 - "guests"
- **User eligibility validated against TAPDB**
- **Will be synchronized with DOD master Directory (CAC cards)**
- **User Properties**
 - "e-mail for life" address
 - Duty e-mail address
 - Ties back to Personnel System (TAPDB)
 - SSN (restricted access)
 - Rank
 - MOS
 - ...

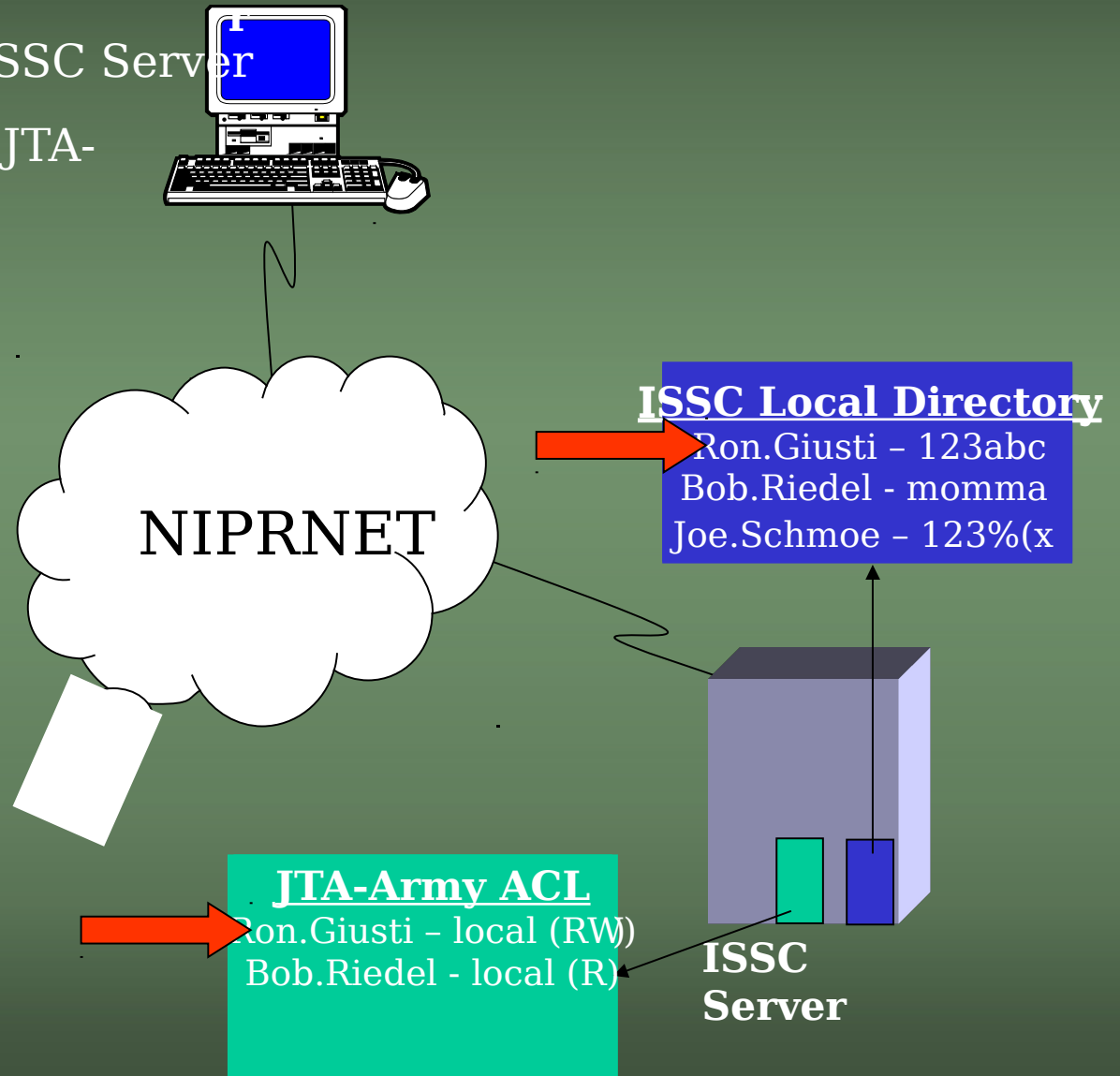
Why use the AKO Directory?

- **User perspective**
 - Single userid, password
 - Single identity
- **Application Perspective**
 - Don't need to manage user credentials
 - Switch from userid/password to PKI done ONCE, by AKO Directory
- **Army Perspective**
 - Single identity
 - Single PKI implementation
 - Enables consolidation of messaging, LAN services



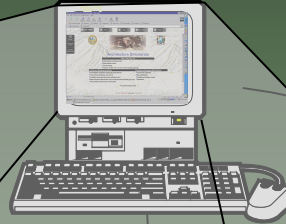
Access Protected Resource: Current way

1. Request ID & PW for ISSC Server
2. Request RW Access to JTA-Army Protected Page

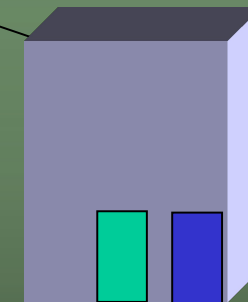


Access Protected Resource: Current way Use

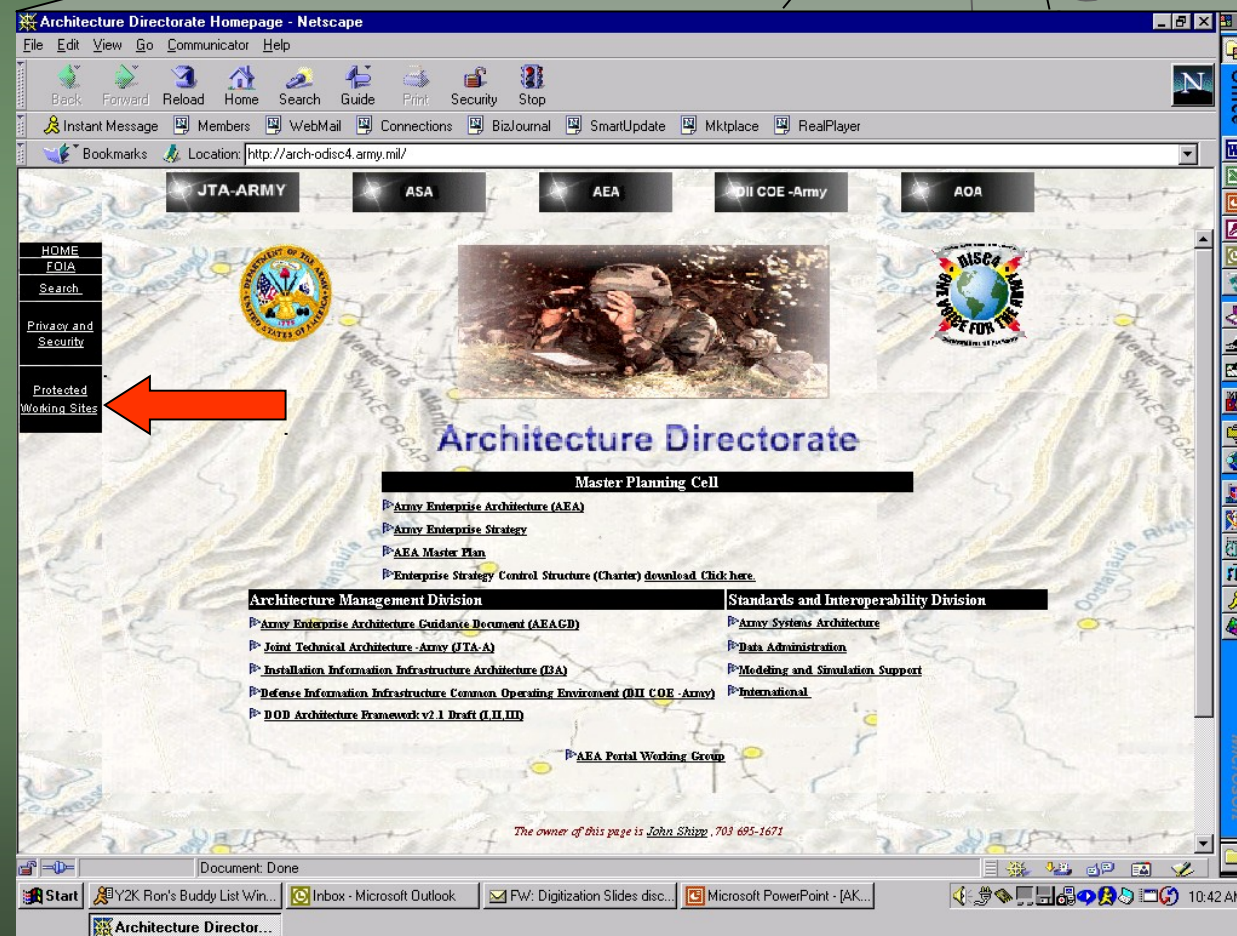
3. Access Architecture Directorate Home page
4. Access Protected Working Sites



<http://arch-odisc4.army.mil/>



ISSC
Server



Access Protected Resource: Current way

3. Access Architecture Directorate Home page
4. Access Protected Working Sites

5. Request JTA-Army Page
6. Authenticate user

7. Confirm access permissions



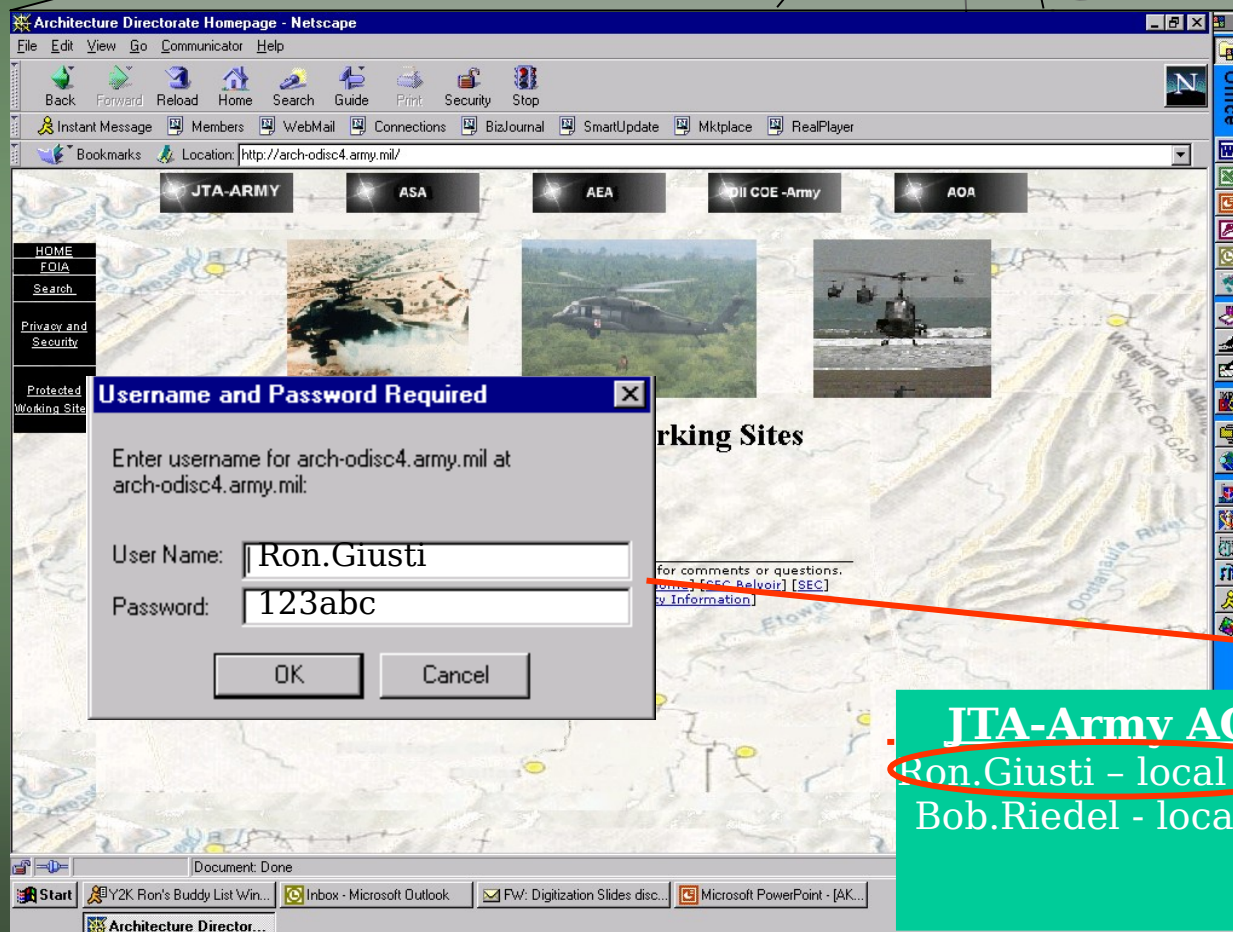
ISSC Local Directory

Ron.Giusti - 123abc
Bob.Riedel - momma
Joe.Schmoe - 123%(x

JTA-Army ACL

Ron.Giusti - local (RW)
Bob.Riedel - local (R)

ISSC Server



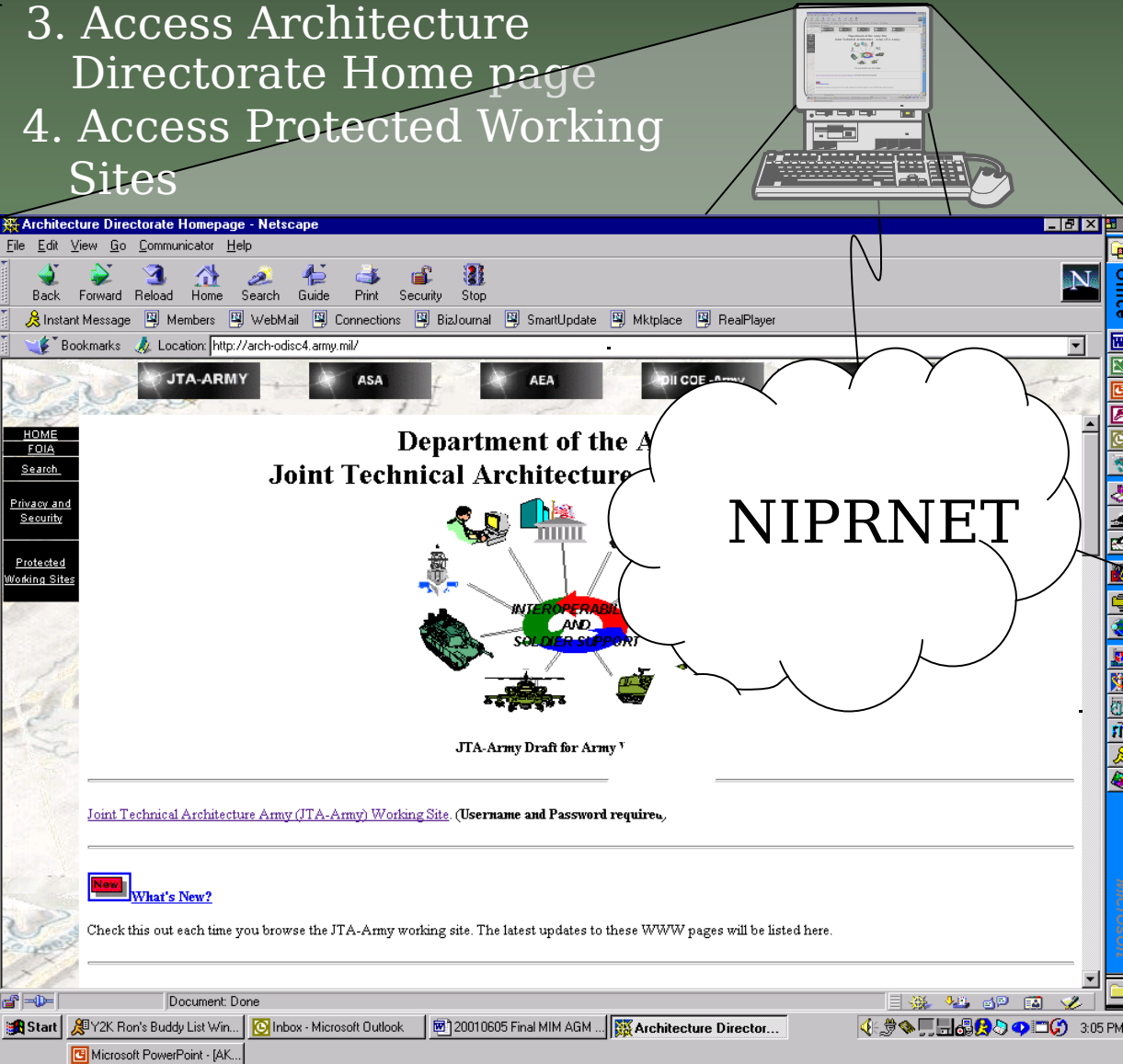
Access Protected Resource: Current way

3. Access Architecture Directorate Home page
4. Access Protected Working Sites

5. Request JTA-Army Page
6. Authenticate user
7. Confirm access permissions

NIPRNET

ISSC
Server

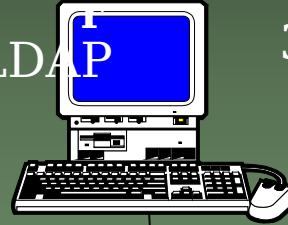


Access Protected Resource: via AKO

Use

1. Configure ISSC Server with LDAP
2. Request ID & PW for AKO Server

3. Request RW Access to JTA-Army Protected Page for AKO ID



AKO LDAP Directory

Bob.Riedel - escargot
Joe.Schmoe - 123%(x
Fred.Snuffy - d8495kf
Mary.Poppins - utopia
Ron.Giusti - marypop

ISSC Local Directory

Ron.Giusti - xxm893
Bob.Riedel - momma
Joe.Schmoe - 123%(x

NIPRNET

LDAP protocol

AKO
Server

ISSC
Server

JTA-Army ACL

Ron.Giusti - local (RW)
Bob.Riedel - local (R)
Ron.Giusti - AKO (RW)



Access Protected Resource: via AKO

Example
Architecture
re
"Portlets"

4. Request JTA-Army
Page

The screenshot shows a Netscape browser window titled "The Army Portal - Netscape". The address bar displays "https://". The page features a header with the "ako The Army Portal" logo and a navigation bar with tabs: Home, Personalize, Reference, and Webmail. A welcome message reads "Welcome to The Army Portal, Ronald G. [Name] 2001".

The main content area is divided into several portlets:

- My Army Portal:** Contains links for Edit Content, Edit Layout, Edit Personal Info, and Change Password.
- AKO White Pages:** Includes input fields for First Name and Last Name, a "seek" button, and a link to "Advanced".
- Search:** Features a search bar, radio buttons for "Army Web Sites" (selected), "Acronym Finder", "Internet", and "Dictionary", and a "seek" button.
- Early Bird News:** Lists "Public Arch Web Site" and "Protected Arch" sections, each containing links to "DISC4 Architecture Directorate", "TRADOC", "Ft. Gordon", and "Ft. Detrick".
- Task Force XXI:** Lists several news items, including "Sylvester to take command in Bosnia (07/18)", "PAC-3 intercept test a partial success (07/17)", "Korea - 50 years ago this week, July 19-25 (07/17)", "Vietnam hero awarded Medal of Honor (07/17)", and "Army inducts soldiers from 3 eras in Hall of Heroes (07/17)".
- AKO Concept Search:** Includes a "NEW!" badge and the "ako" logo.

A red callout box with the text "4. Request JTA-Army Page" has an arrow pointing to the "JTA-Army IA/ESM WSTAWG I3A Repository" link in the "Protected Arch" section of the "Early Bird News" portlet.

The taskbar at the bottom shows the Start button, several open applications (Inbox - Microsoft Outlook, There's a small chance I'll..., The Army Portal - Net..., Microsoft PowerPoint - [AK...]), and the system clock showing 2:59 PM.

Access Protected Resource: via AKO

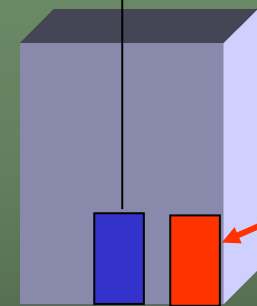
5. Authenticate user
6. Confirm access permissions

AKO LDAP Directory

- Bob.Riedel - escargot
- Joe.Schmoe - 123%(x
- Fred.Snuffy - d8495kf
- Mary.Poppins - utopia
- Ron.Giusti - marypop



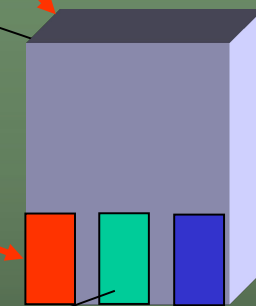
NIPRNET



AKO Server

JTA-Army ACL

- Ron.Giusti - local (RW)
- Bob.Riedel - local (R)
- Ron.Giusti - AKO (RW)



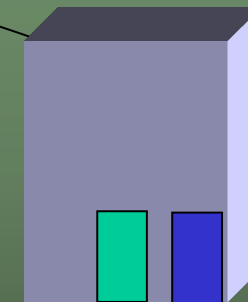
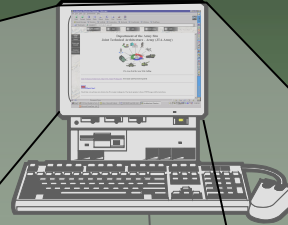
ISSC Server

Access Protected Resource: via AKO

Use

5. Authenticate user

6. Confirm access permissions



ISSC
Server

What does this mean for the “Joint” environment

- **DFAS is currently using our single email for notifications about travel voucher status --- more static environment for them to handle this service**
- **Same concept applies to all DoD provided services such as Tricare**
- **Best case for DoD provided services would be if all services had similar directories --- one place per service to tie into**
- **Could establish mechanism for sharing among the service directories for guest access among the services**